

FortiGate Connector for the HPE VAN SDN - Administration Guide

Version 1.0.

FORTINET DOCUMENT LIBRARY

<http://docs.fortinet.com>

FORTINET VIDEO GUIDE

<http://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

<http://cookbook.fortinet.com/how-to-work-with-fortinet-support/>

FORTIGATE COOKBOOK

<http://cookbook.fortinet.com>

FORTINET TRAINING SERVICES

<http://www.fortinet.com/training>

FORTIGUARD CENTER

<http://www.fortiguard.com>

END USER LICENSE AGREEMENT

<http://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdocs@fortinet.com



Thursday, December 10, 2015

FortiConnector for HPE VAN SDN Controller- Administration Guide

TABLE OF CONTENTS

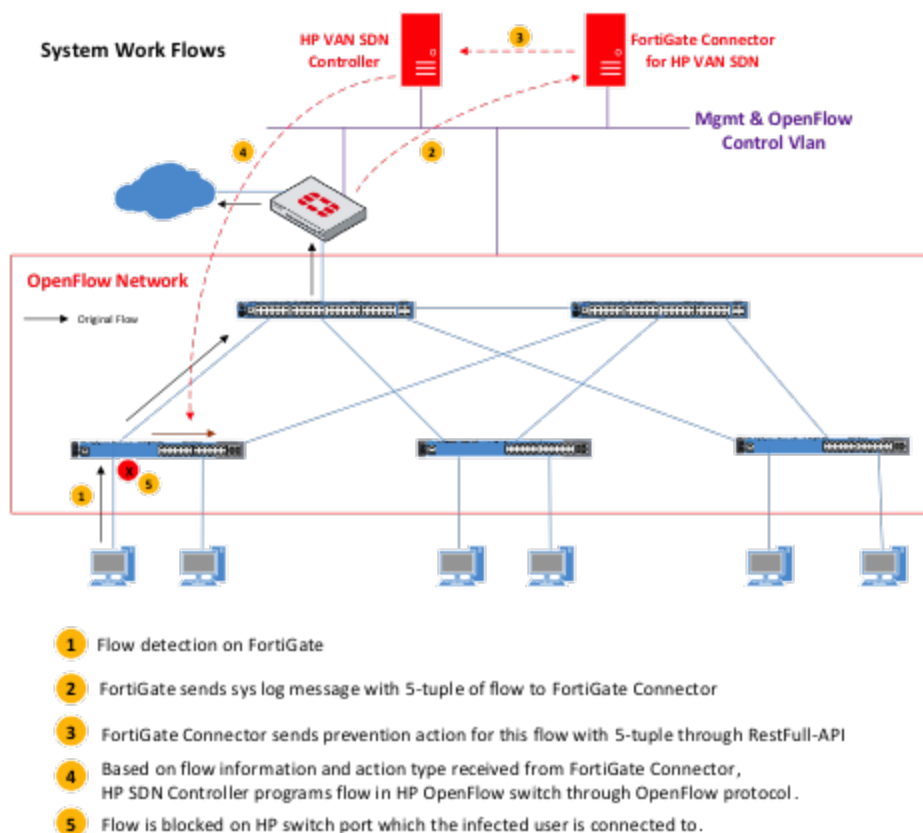
Change Log	4
Overview	5
Licensing	5
Features	5
Supported Products	6
FortiGate products	6
HP products	6
Prerequisites	6
Installation	8
Change Default root password	8
Change default IP address	8
Change default GUI management credential	8
Set system clock	9
Login Page	9
Configuration Page	10
Starting the FortiGate Connector	11
Stopping the FortiGate Connector	11
Clear the configuration and stop FortiGate Connector	12
Supported use scenarios	13
Basic Troubleshooting	14
Verify flow pushed by FortiGate Connector on HP SDN Controller	14
Verify flow pushed by FortiGate Connector on HP switch	15

Change Log

Date	Change Description
2015-12-10	Initial Release

Overview

FortiGate Connector for HP Van SDN version 1.0 is the Fortinet solution that provides the necessary preventative action to isolate an endpoint from the rest of the network in case it generates malicious traffic such that from an exploit or from botnet command and control. The purpose of this preventative action is to block the user's traffic as close as possible to the connected switch and therefore prevent the spread of attack to the rest of the network.



Licensing

FortiGate Connector for HP VAN SDN is free of charge for Fortinet customers. Your FortiGate must be registered with FortiCare at <https://support.fortinet.com>. Also, you will need to agree with the general Fortinet license agreement. The agreement can be found at <http://www.fortinet.com/doc/legal/EULA.pdf>.

Features

The FortiGate Connector for HP Van SDN version 1.0 supports the following functions:

- Preventative action based on the results of scans by the AntiVirus engine
- Preventative action based on the results of scans by the Intrusion Prevention System (IPS) engine

- Preventative action based on scans set by parameters in the Application Control Profile
- Preventative action based on scans set by parameters in the Web Filter Security Profile

Supported Products

FortiGate products

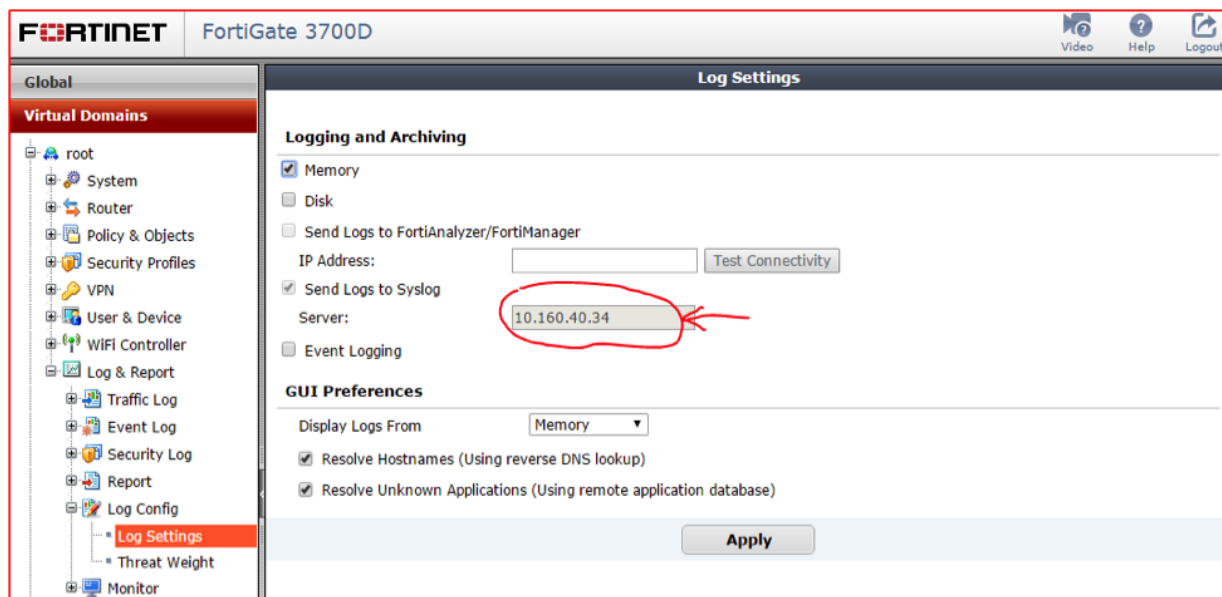
- All physical FortiGate devices running:
 - FortiOS 5.2
 - FortiOS 5.4
- A versions of FortiGate-VM running:
 - FortiOS 5.2
 - FortiOS 5.4

HP products

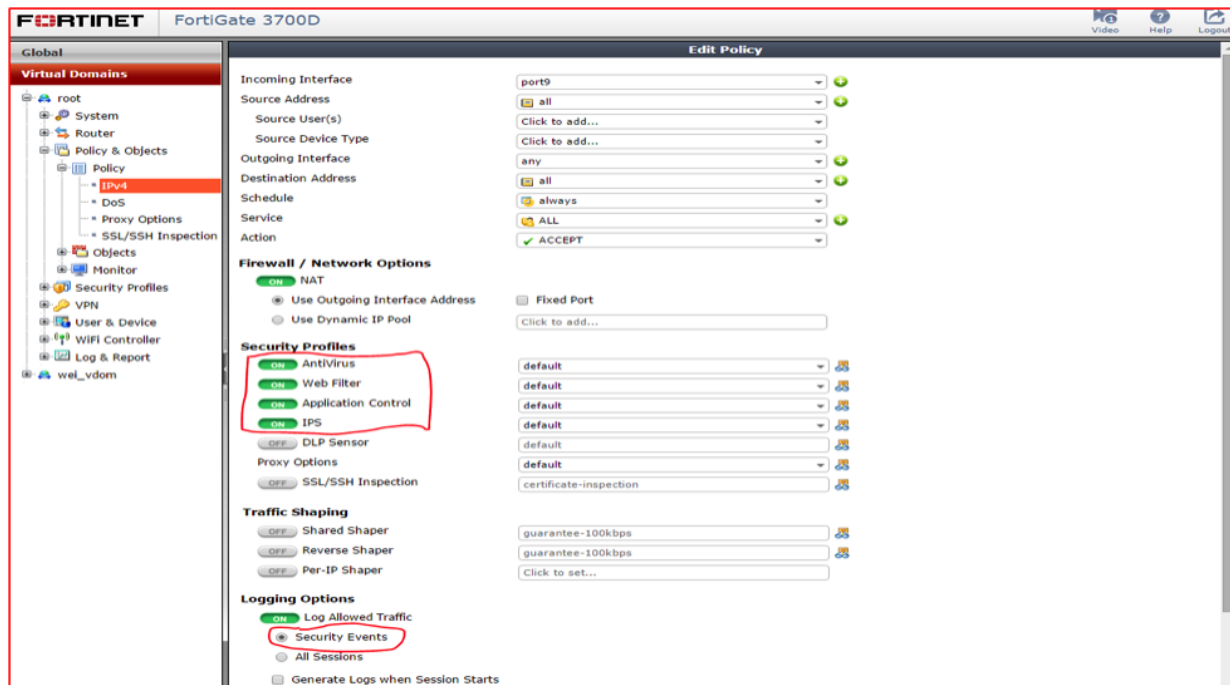
- HP VAN SDN Controller version: 2.5.15
- HP Switch version: KA.15.18.0006

Prerequisites

- The FortiGate Connector IP address should be entered in the field for the Syslog server IP address on the FortiGate.



- In order for the FortiGate Connector to make use of the **Security Profiles**, the profiles, as well as the **Security Events** option, need to be enabled on the FortiGate.



Installation

FortiGate Connector for HP VAN SDN is packaged in a VmWare OVF file. In order to deploy FortiConnector for HPE VAN SDN Controller the file `FortiConnector_v1.0.ovf` on VMware ESXi 5.5 needs to be used.

Change Default root password

The default root credentials for FortiGate Connector for HP VAN SDN are:

- User name = `forticonnector`
- Password = `fortinet`

The user name cannot be changed but the password can be changed using the following steps:

1. Use the default root credentials to login to the FortiGate Connector.
2. At the prompt execute the following command:
`passwd`
The results will be:
`Changing password for forticonnector.`
`(current) UNIX password:`
3. Enter the current password which should be the default password `fortinet`.
`Enter new UNIX password:`
4. Enter the new password that you want to use.
`Retype new UNIX password:`
5. Verify the password by retyping it. If all done correctly the result should be:
`passwd: password updated successfully`

Change default IP address

The default IP address is `192.168.99.1`.

The IP address can be changed using the following command:

```
sudo ifconfig eth0 <new_IP_address> netmask <new_subnet_mask>
```

Change default GUI management credential

The default login credentials of the GUI management interface are:

- User name = admin
- Password = admin

The user name and password can be changed using the following steps:

1. Use root credential to login FortiGate Connector console
2. Use the `cd` command to go to the directory with the config folder
`cd /home/forticonnector/workspace/sdn_hp/config`
3. Use `vi` to open the password file using the following command:
`vi fsdn_passwd.text`
4. Use `vi` to modify user name and password.

Set system clock

The system clock needs to be set accurately to make sure it is in sync with the clock in the HP VAN SDN controller.

To configure time zone:

```
sudo dpkg-reconfigure tzdata
sudo /etc/init.d/cron stop
sudo /etc/init.d/cron start
```

To configure clock:

Use the following command to manually set a specific date and time:

```
sudo date -set="2015-12-09 13:52:52"
```


Option:

You can use the standard Ubuntu method to install the NTP daemon and enable NTP to sync the system clock with a time server on the Internet. The advantage with this method is that once set up, you don't have to worry if your clock speed is slower or faster than the controller's. You can install the daemon with:

```
sudo apt-get install ntp
```

Login Page

Logging into the GUI management interface is done by using the HTTPS prefix and the device's address in your browser as a URL. The default URL would be `https://192.168.1.99`. If the default IP address is still in use but your computer's address on a different subnet you will need to temporarily change the IP address of your computer to be on the same subnet.

 **FortiGate Connector**

Username:


Password:

[LOGIN](#)

Configuration Page

Once on the configuration page of the the FortiGate Connector there are some configuration settings that may need to be changed to integrate the device and set the preferences for your network:

- Configure the IP address for the HP VAN SDN Controller
- Configure the access credentials for the HP VAN SDN Controller
- Configure Action type for each security type
- Configure flow Timeout value for each security type.(Enter 0 for default timeout value 600 seconds)

 **FortiGate Connector**
HP VAN SDN ▾ Logout

HP VAN SDN Controller

IP Address:
 Username:
 Password:

Security Type	Event	SDN Action	Timeout(sec)
AntiVirus	Severe virus detected	<input type="text" value="Prevention"/>	<input type="text" value="3600"/>
Application Control	Detected application to be blocked	<input type="text" value="Prevention"/>	<input type="text" value="600"/>
Intrusion Protection	Attack of intrusion detected	<input type="text" value="Prevention"/>	<input type="text" value="3600"/>
Web Filter	Access to blocked URL	<input type="text" value="None"/>	<input type="text" value="300"/>

Event Logs

Welcome!
 The FortiSDN App is an application providing SDN security for HP environments. As SDN matures and deployment is considered for enterprises production data centers, the Fortinet and HP SDN integration enables security scenarios between Fortinet's FortiGate Next Generation Firewall and the HP VAN SDN Controller. The application is designed to extend the agility and operational

Starting the FortiGate Connector

Once the correct settings have been configured select the **Run** button. The application should start. When the **Status** indicator displays “**running ...**”, it means the FortiGate Connector is ready to receive Syslog information from the FortiGate and to push the flows to the HP VAN SDN Controller.

The screenshot shows the FortiGate Connector web interface. At the top, there is a green header bar with the title "FortiGate Connector" and a "Logout" button. Below the header, the "HP VAN SDN Controller" section contains input fields for "IP Address" (10.160.40.33), "Username" (sdn), and "Password" (masked with asterisks). Below these fields is a table with four columns: "Security Type", "Event", "SDN Action", and "Timeout(sec)". The table has four rows of configuration data. At the bottom of this section are "Run", "Clear", and "Stop" buttons. Below the configuration section is the "Event Logs" section, which contains a scrollable text area with a welcome message. At the very bottom, a yellow status bar displays "Status: running...".

Security Type	Event	SDN Action	Timeout(sec)
AntiVirus	Severe virus detected	Prevention	3600
Application Control	Detected application to be blocked	Prevention	600
Intrusion Protection	Attack of intrusion detected	Prevention	3600
Web Filter	Access to blocked URL	None	300

Welcome!
The FortiSDN App is an application providing SDN security for HP environments. As SDN matures and deployment is considered for enterprises production data centers, the Fortinet and HP SDN integration enables security scenarios between Fortinet's FortiGate Next Generation Firewall and the HP VAN SDN Controller. The application is designed to extend the agility and operational

Status: running...

Stopping the FortiGate Connector

To stop the FortiGate Connector, select the **Stop** button. The **Status** indicator will display "**stopped**". This means FortiGate Connector has stopped all previously pushed flows from being sent to the HP VAN SDN Controller, but the all the configurations are unchanged and maintained.

FortiGate Connector

HP VAN SDN Logout

HP VAN SDN Controller
IP Address: 10.160.40.33
Username: sdn
Password: *****

Security Type	Event	SDN Action	Timeout(sec)
AntiVirus	Severe virus detected	Prevention	3600
Application Control	Detected application to be blocked	Prevention	600
Intrusion Protection	Attack of intrusion detected	Prevention	3600
Web Filter	Access to blocked URL	None	300

Run Clear Stop

Event Logs

Welcome!
The FortiSDN App is an application providing SDN security for HP environments. As SDN matures and deployment is considered for enterprises production data centers, the Fortinet and HP SDN integration enables security scenarios between Fortinet's FortiGate Next Generation Firewall and the HP VAN SDN Controller. The application is designed to extend the agility and operational

Status: stopped

Clear the configuration and stop FortiGate Connector

To clear the FortiGate Controller, select the **Clear** button. The application will stop and configurations will be cleared. When the **Status** indicator displays “**clearing...stopped**”, it means the FortiGate Connector has stopped all previously pushed flows from being sent to the HP VAN SDN Controller, and has cleared previous configurations.

FortiGate Connector

HP VAN SDN Logout

HP VAN SDN Controller
IP Address:
Username:
Password:

Security Type	Event	SDN Action	Timeout(sec)
AntiVirus	Severe virus detected	None	<input type="text"/>
Application Control	Detected application to be blocked	None	<input type="text"/>
Intrusion Protection	Attack of intrusion detected	None	<input type="text"/>
Web Filter	Access to blocked URL	None	<input type="text"/>

Run Clear Stop

Event Logs

Welcome!
The FortiSDN App is an application providing SDN security for HP environments. As SDN matures and deployment is considered for enterprises production data centers, the Fortinet and HP SDN integration enables security scenarios between Fortinet's FortiGate Next Generation Firewall and the HP VAN SDN Controller. The application is designed to extend the agility and operational

Status: clearing... stopped

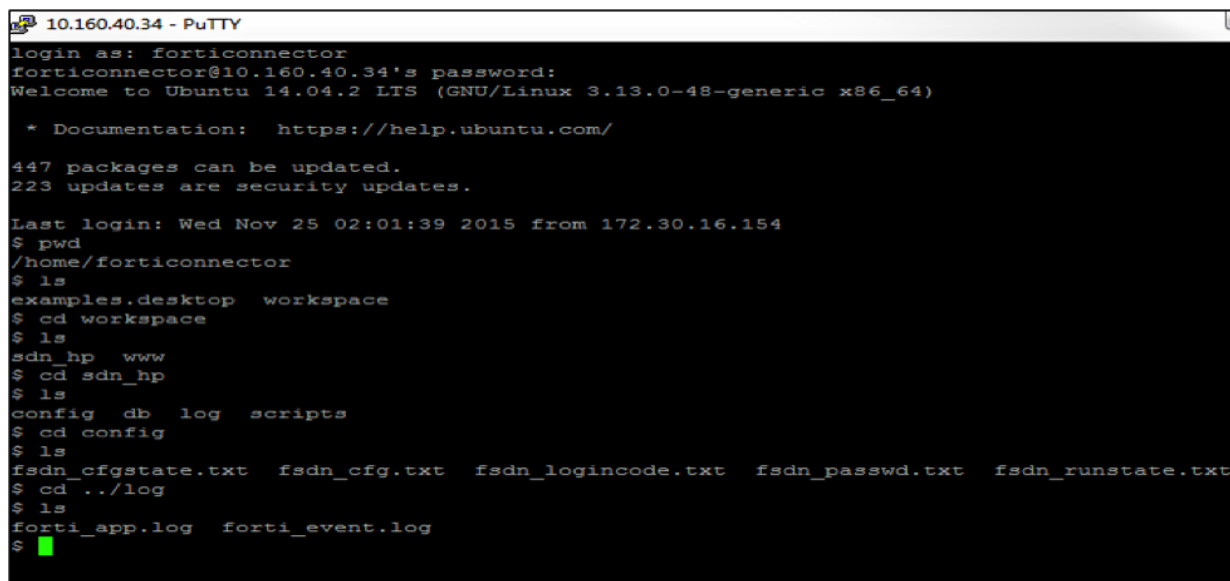
Supported use scenarios

- When a user sends a malware file through the network and the FortiGate detects it, the FortiGate Connector will push the flow, along with the user's source IP address and a block action, to the HP SDN controller. The user port of the HP switch will then block all subsequent traffic from this user's IP address.
- When a user generates a botnet command to attack the network that is detected by the FortiGate IPS engine, the FortiGate Connector will push the flow, along with the user's source IP address and a block action, to the HP SDN controller. The user port of the HP switch will then block all subsequent traffic from this user's IP address.
- When a user initiates an application prohibited by the Application Control profile on the FortiGate, the FortiGate Connector will push this application flow, along with the user's source IP address, the destination IP address, the listening port number, and a block action command to the HP SDN controller. The user port of the HP switch then blocks all matching application traffic from this user's IP address. Other traffic from the user is not affected.
- When a user tries to access a web site prohibited by the FortiGate's Web Filter profile, the FortiGate Connector will push this web access flow, along with the user's source IP address, the destination IP address of the web site, and a block action command to the HP SDN controller. The user port of the HP switch then blocks all traffic from the user's IP address to the website's IP address. Traffic from the user to other websites is not affected.

Basic Troubleshooting

The following are some quick pieces of information that may be helpful in troubleshooting issues that may come up while administering your FortiGate Connector:

- The configuration file is located in the folder: `/home/forticonnector/workspace/sdn_hp/config/`
 - The file is: `fsdn_cfg.txt`.
- Debug messages and event logs are located in the following files:
 - `forti_app.log`
 - `forti_envent.log` (contains events only)
- The syslog messages from the FortiGate are located in the folder: `/var/log/syslog`.



```
10.160.40.34 - PuTTY
login as: forticonnector
forticonnector@10.160.40.34's password:
Welcome to Ubuntu 14.04.2 LTS (GNU/Linux 3.13.0-48-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

447 packages can be updated.
223 updates are security updates.

Last login: Wed Nov 25 02:01:39 2015 from 172.30.16.154
$ pwd
/home/forticonnector
$ ls
examples.desktop  workspace
$ cd workspace
$ ls
sdn_hp  www
$ cd sdn_hp
$ ls
config  db  log  scripts
$ cd config
$ ls
fsdn_cfgstate.txt  fsdn_cfg.txt  fsdn_logincode.txt  fsdn_passwd.txt  fsdn_runstate.txt
$ cd ../log
$ ls
forti_app.log  forti_event.log
$
```

Verify flow pushed by FortiGate Connector on HP SDN Controller

In order to verify flows pushed by the FortiGate to the HPE VAN SDN Controller, navigate to the flow page on the HPE VAN SDN Controller.

HP VAN SDN Controller

15
sdn

General

Alerts

Applications

Configurations

Audit Log

Licenses

Team

Support Logs

OpenFlow Monitor

OpenFlow Topology

OpenFlow Trace

OpenFlow Classes

Packet Listeners

Flows for Data Path ID: 00:01:10:60:4b:b6:2a:40

Summary

Ports

Flows

Groups

Table ID	Priority	Packets	Bytes	Match	Actions/Instructions	Flow Class ID
n/a	31000	869	55616	eth_type: arp	output: CONTROLLER output: NORMAL	com.hp.sdn.arp.copy
n/a	60000	0	0	eth_type: bddp	output: CONTROLLER	com.hp.sdn.bddp.steal
n/a	31500	0	0	eth_type: ipv4 ip_proto: udp udp_src: 67 udp_dst: 68	output: CONTROLLER output: NORMAL	com.hp.sdn.dhcp.copy
n/a	31500	246	85116	eth_type: ipv4 ip_proto: udp udp_src: 68 udp_dst: 67	output: CONTROLLER output: NORMAL	com.hp.sdn.dhcp.copy
n/a	65000	43	0	in_port: 1 eth_type: ipv4 vlan_vid: 3 ipv4_src: 30.30.30.40, mask: 255.255.255.255		
n/a	0	7471	1229593		output: NORMAL	com.hp.sdn.ip.normal

Blocked flow from Fortinet Connector

Blocked flow from Fortinet Connector

Verify flow pushed by FortiGate Connector on HP switch

In order to verify flows pushed by the FortiGate to the HPSwitch

1. Login to the HP switch console.
2. Issue the following command:

HP-Switch# show openflow instance aggregate flows

```

Controller ID : 1                               Cookie : 0xffffc0000babadada
Flow Location : Software
Hardware Index: NA
Reason Code   : 10
Reason Description : The action and output port in the rule is invalid or not supported
Actions
  Controller Port
  Normal

Flow 5
Match
Incoming Port : 1
Source MAC : Any
Destination MAC Mask : 0000000-0000000
VLAN ID : 3
Source IP Address : 30.30.30.40/32
Destination IP Address : Any
IP Protocol : Any
Source Port : Any
Ethernet Type : IP
Destination MAC : Any
VLAN Priority : Any
Attributes
Priority : 65000
Hard Timeout : 60 seconds
Byte Count : 0
Controller ID : 1
Flow Location : Hardware
Hardware Index: 0
Reason Code : 12
Reason Description : Rule is in hardware.
Actions
  Drop ← blocked flow programmed by HP SDN on switch

Flow 6
Match
Incoming Port : Any
Source MAC : Any
Destination MAC Mask : 0000000-0000000
VLAN ID : Any
Source IP Address : Any
Destination IP Address : Any
IP Protocol : Any
Source Port : Any
Ethernet Type : Any
Destination MAC : Any
VLAN Priority : Any
IP ToS Bits : Any
Destination Port : Any

```



FORTINET®

High Performance Network Security



Copyright© 2015 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.